PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Chang et al. (SANDP015) Conf. No. 7791

Serial No. 10/092,049 Group Art Unit: 2132

Filed: March 4, 2002 Examiner: Lemma

For: Implementation of Storing Secret Information in Data Storage Reader Products

APPELLANTS' BRIEF

Commissioner for Patents

Washington, DC 20231

Dear Sir:

Appellants respectfully present their brief in support of their appeal of the final rejection of claims in this case. The Notice of Appeal was filed on September 18, 2006, as indicated on the date of the automated receipt from the Patent and Trademark Office.

Real Party in Interest

The real party in interest in this application is SanDisk Corporation.

Related Appeals and Interferences

The undersigned is aware of no related applications that are currently on appeal or in an interference that would be directly affected by, or themselves directly affect or have a bearing on, this appeal.

Status of the Claims

Claims 1, 3, 5 through 8, 11 through 13, and 17 through 24 were finally rejected in the Office Action of May 16, 2006, and are the subject of the present appeal.

Status of Amendments

No amendment was presented after the final rejection. A Request for Reconsideration was filed on August 17, 2006, but the Examiner did not find the arguments presented to be persuasive.

Summary of the Claimed Subject Matter

Independent claim 1 is directed to a method for accessing encrypted information in a flash memory storage device (512; 612), such as a flash memory card, from a host system (504: 604). According to this invention, in order to access and decrypt that information, a user must both enter an access code via the host system, and also read the flash memory card using a specific reader (508; 628) that stores the encryption key that was used to encrypt the data stored on the flash memory card. As expressed in claim 1, the method of accessing this encrypted information requires the forwarding (712, 716) of the access code from a host system to the reader.[1] In response to the access code being valid (720), an encryption key is obtained from its storage location in the reader (720); this key can then be used to access and decrypt the contents of the flash memory (728).[2]

Independent apparatus claim 13 recites a system that comprises a host system (504; 604), and a flash memory reader (508; 628) coupled to that system. The flash memory reader includes an interface that receives a flash memory storage device, and a reader memory (528; 628) for storing a key.[3] The reader also includes circuitry for accessing encrypted information including

---

[1] Specification of S.N. 10/092,049, *e.g.*, at page 12, lines 4 through 8; page 13, lines 1 through 7; page 14, lines 13 through 20; Figures 5, 6, and 7a (steps 712 and 716).
[2] Specification, *supra*, at page 12, lines 9 through 13; page 13, lines 7 through 9; page 14, line 22 through page 15, line 7; page Figures 5, 6, and 7a (steps 720 and 728), and 7c (steps 754 and 758).
[3] Specification, *supra*, page 11, line 21 through page 12, line 2; page 12, line 28 through page 13, line 5; Figures 5 and 6.

means for receiving an access code from the host system, and means for obtaining the key from the reader memory if that access code is valid. The specification discloses an example of structure for the receiving means and the obtaining means by way of reader firmware (510) that is executed by logic circuitry within the reader (508; 608), for example in connection with a Protected Contents Feature Set[4]. The system of claim 13 and its dependent claims also comprises means for decrypting information stored on the flash memory storage device, where the decrypting is performed using the key obtained from the reader memory. The specification discloses an example of structure for this decrypting means by way of the reader firmware executed by circuitry within the reader,[5] or by way of software executed on the host.[6]

The claimed invention, in both its method and system form, provides important security advantages over conventional secure flash memory systems. These advantages result from the storing of an encryption key on a reader rather than on a host system, in combination with requiring the entry of an access code from the host system in order to access that encryption key. Therefore, in order to access the data stored in the flash memory device, one must have both information that is known to the legitimate user (the access code) and must also have a specific hardware device (the reader containing the encryption key) that is separate from the flash memory card itself. This method greatly increases the security of the encrypted contents of a flash memory device. A thief or other unauthorized user who is in possession of the flash memory storage device cannot access its contents without possession of both the reader storing the key, and also the valid access code necessary to retrieve that key.[7]

---

[4] Specification, *supra*, page 12, lines 22 through 24; page 13, lines 7 through 9; page 18, lines 4 through 10; page 27, lines 19 through 25; Figures 9a *et seq.*

[5] Specification, *supra*, page 16, lines 14 through 16.

[6] Specification, *supra*, page 33, lines 14 through 19 (original claims 20 and 21).

[7] Specification, *supra*, page 7, lines 4 through 15; page 10, line 25 through page 11, line 4.

Grounds of Rejection to Be Reviewed On Appeal

The rejection of claim 1 and its dependent claims

Claims 1, 3, 5 through 8, 11 and 12 were all finally rejected under §103 as unpatentable over the Jones et al. reference[8] in view of the Tatebayashi et al. reference[9]. The Examiner asserted that the Jones et al. reference teaches all of the steps of independent method claim 1 except for the step of inserting a flash memory device into a reader. However, the Examiner asserted that the Tatebayashi et al. reference teaches such inserting, and that it would have been obvious to modify the Jones et al. reference to include that additional step, in order to authenticate the flash memory with the reader.[10]

In response to Appellants' arguments in the Request for Reconsideration Under Rule 116 filed August 17, 2006, the Examiner stated that it would have been obvious to combine the teachings of the Tatebayashi et al. reference regarding the inserting of a flash memory storage device into a reader, into the teachings of the Jones et al. reference (in which the memory array and encryption mechanism reside in the same physical unit), "in order to authenticate the flash memory with the reader".[11]

Specific limitations of the dependent claims were found by the Examiner to be present in the references, or obvious therefrom.

The rejection of claim 13 and its dependent claims

Independent apparatus claim 13 and its dependent claims 17 through 24, were finally rejected, under §103, as unpatentable over the combination of the Jones et al. and Tatebayashi et al. references on similar grounds as asserted against claim 1. Specific limitations of the dependent claims were found by the Examiner to be present in the references, or obvious therefrom.

---

[8] U.S. Patent No. 6,623,637, issued April 22, 1997 to Jones et al.

[9] U.S. Patent No. 6,859,535, issued February 22, 2005 to Tatebayashi et al., from an application filed October 15, 1999.

[10] Office Action of May 16, 2006, pages 2 through 4.

The comments made by the Examiner in the Advisory Action of August 30, 2006, in response to Applicants' arguments, were also applied against these apparatus claims 13 and 17 through 24.

Argument

It is axiomatic, in the patent law, that a *prima facie* obviousness determination of patent claims requires teachings from the prior art itself to appear to have suggested the claimed subject matter to a person of ordinary skill in the art.[12] If the Examiner fails to establish such a *prima facie* case, the obviousness rejection is improper and should be overturned on appeal.[13] If the suggestion or motivation to combine references is not supported by evidence, the combination is therefore simply an improper use of the inventor's own teachings in hindsight.[14]

Claim 1 and its dependent claims

Appellants respectfully submit that the Examiner has failed to establish a *prima facie* case of obviousness relative to claim 1, because there is no suggestion from the prior art to combine the teachings of the Tatebayashi et al. reference with those of the Jones et al. reference, in such a manner as to reach independent claim 1. Appellants therefore submit that the final rejection of claim 1 and its dependent claims is in error and should be reversed.

The Jones et al. reference is directed to a memory card on which encrypted content can be stored, and which can interface to a host personal computer, for example by way of a PCMCIA interface.[15] This detachable "Secure Memory Card" (100)[16] includes both a non-volatile flash memory array (150)[17] and also a smartcard integrated circuit (250).[18] The

---

[11] Advisory Action of August 30, 2006.
[12] *In re Rijckaert*, 9 F.3d 1531, 1532, 28 USPQ2d 1955, 1956 (Fed. Cir. 1993).
[13] *Rijckaert, supra.*
[14] *In re Dembiczak,* 175 F.3d 994, 999, 50 USPQ3d 1614 (Fed. Cir. 1999) ("Combining prior art references without evidence of such a suggestion, teaching, or motivation simply takes the inventor's disclosure as a blueprint for piecing together the prior art to defeat patentability -- the essence of hindsight.").
[15] Jones et al., *supra,* column 2, lines 10 through 23.
[16] Jones et al., *supra,* Figure 2.
[17] Jones et al., *supra,* column 3, lines 50 through 67.
[18] Jones et al., *supra,* column 5, lines 1 through 19.

smartcard integrated circuit includes the processor and memory necessary to operate as a "secret key information substorage system" within the detachable memory card.[19] As disclosed in the Jones et al. reference, the user of the personal computer who wishes to access a partition in the memory array connects the detachable memory card (embodying both the smartcard integrated circuit and the flash memory array) to a host personal computer, for example at a PCMCIA port, and provides a password via the detachable memory card via the host personal computer; if the password is valid, access to the protected partition is granted by the smartcard integrated circuit in the detachable memory card.[20]

The Jones et al. reference falls short of the requirements of claim 1 because it does not disclose the step of inserting a flash memory storage device into a reader. The reference fails to disclose this step because its flash memory storage array and its smartcard integrated circuit (*i.e.,* the function that performs such steps as controlling secure access to protected information stored in the flash memory storage array) are embodied within the same physical card, namely the detachable PCMCIA smart memory card, which is itself insertable into and removable from the host personal computer.[21] Accordingly, the Jones et al. reference does not disclose a reader that is separate and separable from the flash memory storage device. Rather, the smart memory card 100 of the reference, which contains both memory array 150 (asserted as the flash memory storage device of claim 1) and smartcard integrated circuit 250 (asserted as the reader of claim 1), is inserted as a whole into the host personal computer. The Examiner agrees with this shortfall of the Jones et al. reference relative to claim 1.[22]

The Examiner asserts, however, that the Tatebayashi et al. reference provides this missing teaching, in connection with its disclosure of the inserting of a memory card (200) into a memory card reader (400) that stores a key used to decrypt the contents stored on the memory

---

[19] Jones et al., *supra,* column 5, lines 1 through 19.
[20] Jones et al., *supra,* column 8, line 52 through column 9, line 25.
[21] Jones et al., *supra,* column 3, lines 16 through 49.
[22] Advisory Action, *supra,* page 2 ("The other argument presented by the applicant is that Jones et al. the reference on record does not disclose the limitation 'inserting the flash memory storage device into the reader.' Examiner agreed with this particular applicant's argument. In other words Applicant argument is not only persuasive but correct that this limitation is not taught/disclosed in the [Jones] reference.")

card.[23] The Examiner also asserts that the skilled artisan would be motivated to combine this teaching with the Jones et al. reference, in order to "authenticate the flash memory with the reader" in the Jones et al. system.[24]. Appellants disagree with the Examiner, and assert that there is no such motivation present in the prior art, especially the Tatebayashi et al. reference itself, to make this combination.

First, Appellants submit that the motivation alleged by the Examiner is in error because that specific motivation is not present in the alleged combination of references. There is no need to "authenticate the flash memory with the reader" according to the teachings of the Jones et al. reference. This is because the flash memory and the alleged reader (*i.e.,* the smartcard integrated circuit) are embodied into the same physical object – the detachable PCMCIA card. The Jones et al. reference nowhere discloses that its flash memory and its smartcard integrated circuit are physically separated from one another at any time after manufacture. Indeed, the reference nowhere mentions that the two are even physically separable from one another (short of destroying the memory card, of course). Once these elements are combined at manufacture, the flash memory and smartcard integrated circuit of course are physically associated with one another, and will remain so. There will never be a need, according to the Jones et al. reference, for the smartcard integrated circuit to authenticate a different flash memory, nor for the flash memory to authenticate a different smartcard integrated circuit. Accordingly, according to the Jones et al. reference, there is no need whatsoever to "authenticate the flash memory with the reader", and therefore no motivation to combine the Tatebayashi et al. teachings into the Jones et al. method of operation. Appellants therefore respectfully submit that the motivation alleged by the Examine for combining the applied references is in fact not present, and therefore that the final rejection of claim 1 and its dependent claims is in error.

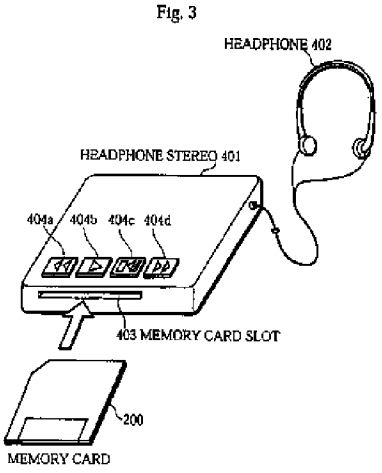
Secondly, Appellants submit that there is in fact no motivation from the prior art to combine the teachings of the Tatebayashi et al. reference with those of the Jones et al. reference for any rational reason. As discussed above, in order to modify the teachings of the Jones et al.

---

[23] Advisory Action, *supra*, *citing* Tatebayashi et al., *supra,* at column 18, lines 9 through 29; Figures 2, 6, 8, and 18.

reference to reach the method of claim 1, one would have to be motivated to modify the Jones et al. detachable memory card so that the flash memory array could be separated from the smartcard integrated circuit, so that it could be inserted into a "reader" as required by claim 1. Considering the teachings of the Jones et al. reference itself regarding the convenient "credit-card" size of the detachable PCMCIA memory card,[25] there is little motivation from the Jones et al. reference itself to cause its memory card to be separable from its PCMCIA card (with smartcard integrated circuit).

Nor does the Tatebayashi et al. reference provide any motivation to the skilled artisan to modify the Jones et al. reference to separate its flash memory storage array separate from the rest of the detachable memory card. This is apparent from the purpose of the system and method disclosed in the Tatebayashi et al. reference, namely a digital rights management system for flash memory cards.[26] In this regard, the "reader" disclosed by the Tatebayashi et al. reference is a stand-alone memory card reader, in the sense that the reader is not connected to the host computer when it is accessing the contents of the memory card. Figure 3 of the reference is instructive in this regard, as it shows reader 400 in the form of a headphone stereo 401[27]:



[24] Advisory Action, *supra*.
[25] Jones et al., *supra*, column 3, lines 50 through 55.
[26] *See* Tatebayashi et al., *supra*, column 1, lines 9 through 25.
[27] *See also* Tatebayashi et al., *supra*, column 8, lines 35 through 43.

How would this portable stereo system motivate the skilled artisan to separate the flash memory from the smartcard integrated circuit in the PCMCIA card of the Jones et al. reference? Appellants can envision no way in which it does. Furthermore, there is no teaching in the Tatebayashi et al. reference regarding the connecting of this reader to a host personal computer to read the memory card. Nor does the Tatebayashi et al. reference disclose the forwarding of an access code to this headphone stereo "reader", or to any other card reader, responsive to which an encryption key can be obtained from the reader. The skilled artisan would therefore have no reason, from the Tatebayashi et al. reference, to modify the teachings of the Jones et al. reference so that its flash memory storage device becomes insertable into its PCMCIA card.

It is impermissible to use hindsight reconstruction to pick and choose among teachings in the prior art, in order to piece together a claimed invention for purposes of finding claims obvious.[28] Because such suggestion or motivation is lacking in this case, it is apparent to Appellants that the rejection of claim 1 and its dependent claims is based on such an impermissible "picking and choosing" of teachings from the Tatebayashi et al. reference, without regard to the context of the Tatebayashi et al. reference itself. Appellants therefore submit that the final rejection of claim 1 and its dependent claims, as unpatentable over the combination of the Jones et al. and Tatebayashi et al. reference, could only have been made through the improper hindsight use of Appellants' own teachings.

Appellants further submit that the differences between the invention of claim 1 and its dependent claims, and the prior art as properly combinable, are sufficiently substantial and important as to support a finding that these claims are patentable. As discussed above, the method of claim 1 and its dependent claims requires the inserting of a flash memory device into a reader, forwarding an access code from the host system to the reader to obtain a key from the reader, and decrypting the information on the flash memory storage device using that key. Accordingly, to access the contents of the flash memory storage device according to the invention, one must have both a valid access code that is forwarded to the reader, and also must

---

[28] *In re Fritch*, 972 F.2d 1260, 23 USPQ2d 1780 (Fed. Cir., 1992); *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

have the reader that contains the encryption key according to which the contents on the flash memory storage device are encrypted. This combination provides important security advantages over conventional secure flash memory systems, because a thief or other unauthorized user possessing the flash memory storage device cannot access its contents without possession of both the reader with the key, and also the valid access code required to retrieve that key.

The two levels of security provided by this invention are a substantial improvement over the single levels of security provided by the Jones et al. and Tatebayashi et al. references. The Jones et al. reference provides only a password security mechanism:

> It is important to observe that the data stored in a protected partition within the memory card 100 is available only to those who possess both the card and the password. Neither possession of the card without knowledge of the password, nor knowledge of the password without physical possession of the card, will be sufficient to obtain access to the data.[29]

Nothing in the Jones et al. reference suggests that this password-security scheme is in any way inadequate, or ought to be improved upon. The Tatebayashi et al. reference gives no indication that its scheme of a memory card and reader mutually authenticating one another is insufficient; rather, the reference indicates that possession of an authentic reader for an authentic card serves the desired security purpose for access to the card contents, namely preventing illegally obtained contents from being reused.[30] Neither reference suggests providing an additional level of security.

Accordingly, Appellants submit that the method of claim 1 provides an important second level of security that is not provided or suggested by the applied references. The Jones et al. reference requires knowledge of the password and possession of the card to access the card contents; this would not be sufficient for access according to the method of claim 1, because possession of the separate reader into which the flash memory storage device is inserted, and which stores the encryption key, is also required. On the other hand, the Tatebayashi et al.

---

[29] Jones et al., *supra,* column 8, lines 35 through 41.
[30] Tatebayashi et al., *supra,* column 2, lines 18 through 37; column 18, lines 5 through 29; column 50, lines 50 through 58; column 51, lines 16 through 27.

reference requires possession of the memory card and possession of the reader; this would not be sufficient for access according to the method of claim 1, because knowledge of the access code and providing that valid access code to the reader from a host system is also required, according to the method of claim 1. The substantial difference between the method of claim 1 and the contents of the prior art, and the resulting improvement in security, is indicative of the patentability of claim 1 and its dependent claims.[31]

For these reasons, Appellants submit that the final rejection of claim 1 and each of its dependent claims 3, 5 through 8, 11 and 12 is in error and should be reversed.

Claim 13 and its dependent claims

Appellants respectfully submit that the Examiner has also failed to establish a *prima facie* case of obviousness relative to claim 13, because there is no suggestion from the prior art to combine the teachings of the Jones et al. and Tatebayashi et al. references so as to reach the system of independent claim 13. Appellants therefore submit that the final rejection of claim 13 and its dependent claims is in error and should be reversed.

As previously discussed, the Jones et al. reference is directed to a memory card on which encrypted content can be stored, and which can interface to a host personal computer, for example by way of a PCMCIA interface. This detachable "Secure Memory Card" includes both the non-volatile flash memory array to be accessed, and also the smartcard integrated circuit that serves as a "secret key information substorage system" within the detachable memory card. But the Jones et al. reference does not disclose a flash memory reader that has an interface for receiving a flash memory storage device, as recited in claim 13. This "interface for receiving" is absent from the Jones et al. reference because the flash memory storage array is embodied with its smartcard integrated circuit within a single physical PCMCIA card that is itself detachable from and insertable into the host personal computer.[32] There is no physically separate flash memory reader disclosed in the Jones et al. reference, separate in the sense that a flash memory

---

[31] *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966).

[32] Jones et al., *supra*, column 3, lines 16 through 49.

storage device can be received into an interface of that reader. The Examiner agrees that the Jones et al. reference fails to teach this limitation of claim 13.[33]

As in the case of claim 1, the Examiner asserts that the Tatebayashi et al. reference provides discloses a memory card (200) that is inserted into a memory card reader (400), such that the memory card reader provides an interface for receiving that memory card. In the Tatebayashi et al. reference, as discussed above, the reader stores a key used to decrypt the contents stored on the memory card.[34] The Examiner asserts that the skilled artisan would be motivated to make this combination in order to "authenticate the flash memory with the reader."[35]

Appellants submit that there is no motivation in the prior art, particularly in the Tatebayashi et al. reference, to combine the teachings of the Tatebayashi et al. reference with those of the Jones et al. reference, to reach claim 13.

As discussed above relative to claim 1, Appellants first submit that the motivation alleged by the Examiner is simply not provided by either of the combined references. In the Jones et al. system, there is no need whatsoever to "authenticate the flash memory with the reader", because the flash memory and the alleged reader are at all times within the same single physical PCMCIA card. Indeed, it is not apparent from the Jones et al. reference that its flash memory array and is smartcard integrated circuit are ever physically separated from one another after manufacture of the PCMCIA card, in which case the flash memory array may be directly soldered or otherwise permanently attached within this PCMCIA card, and not received in an interface. And because of this construction, there is never a need for the smartcard integrated circuit within the Jones et al. reference to "authenticate" this flash memory array that it is physically coupled to at all times following manufacture. Therefore, the skilled reader cannot be motivated to combine the Tatebayashi et al. teachings into the Jones et al. system "to authenticate the flash memory with the reader", as asserted by the Examiner. Appellants

---

[33] Advisory Action, *supra,* page 2.

[34] Advisory Action, *supra, citing* Tatebayashi et al., *supra,* at column 18, lines 9 through 29; Figures 2, 6, 8, and 18.

therefore respectfully submit that the motivation alleged by the Examiner for combining the applied references is in fact not present.

Appellants also submit that there is in fact no motivation from the prior art to combine the teachings of the Tatebayashi et al. reference with those of the Jones et al. reference for any rational reason, even beyond that asserted by the Examiner. As discussed above relative to claim 1, in order to arrive at the system of claim 13, the skilled artisan would have to be motivated to modify the Jones et al. detachable memory card to provide an interface to receive a detachable and insertable flash memory array; in other words, the skilled artisan would have to be motivated to go to the trouble of separating the memory array from the smartcard integrated circuit, and to add a physical interface. However, the Jones et al. reference itself teaches that its PCMCIA memory card has a small "credit-card" size,[36] even including the reader. Certainly this portability of the PCMCIA card as it is, including the smartcard integrated circuit, does not lend one the idea to separate the two – indeed, one may surmise that adding the interface required by the claim may actually decrease this small form factor. One therefore gets no motivation from the Jones et al. reference itself to cause its memory card to be separable from its PCMCIA card (with smartcard integrated circuit), and thus no motivation to modify its teachings to provide the interface.

The Tatebayashi et al. reference also lacks such motivation. The stated purpose of the system of the Tatebayashi et al. reference is to provide a digital rights management system for flash memory cards,[37] and discloses a stand-alone memory card reader that is not connected to the host computer when accessing the contents of the memory card. As discussed above relative to claim 1, the example of the reader disclosed by the Tatebayashi et al. reference is a headphone stereo 401.[38] This system provides the skilled artisan with no reason whatsoever to modify the teachings of the Jones et al. reference so that its flash memory storage device becomes insertable into its PCMCIA card.

---

[35] Advisory Action, *supra*.
[36] Jones et al., *supra*, column 3, lines 50 through 55.
[37] *See* Tatebayashi et al., *supra*, column 1, lines 9 through 25.
[38] Tatebayashi et al., *supra*, column 8, lines 35 through 43; Figure 3.

Therefore, because suggestion or motivation to combine these applied references is not present in the prior art, Appellants submit that the final rejection of claims 13 and 17 through 24 under §103 is in error, as based on the improper hindsight use of Appellants' own teachings.[39] Rather, it appears to Appellants that the rejection of claim 13 and its dependent claims was specifically derived by "picking and choosing" teachings from the Tatebayashi et al. reference to combine with the Jones et al. reference, ignoring the context of the Tatebayashi et al. reference and thus ignoring whether the skilled reader would have made the combination. Appellants therefore submit that the final rejection of claim 13 and its dependent claims, as unpatentable over the combination of the Jones et al. and Tatebayashi et al. reference, could only have been made through the improper use of Appellants' own teachings, in hindsight.[40]

Appellants further submit that the differences between the system of claim 13 and its dependent claims, and the prior art as properly combinable, are sufficiently substantial and important as to support a finding that these claims are patentable. Similarly as discussed above relative to claim 1, the system of claim 13 implements two levels of security, as compared with the single levels of security provided by the Jones et al. and Tatebayashi et al. references, requiring both reader memory that stores a key for decrypting information stored on a flash memory device, and also an access code that is received from a host system and that is used to obtain that key from the reader memory. In contrast, the Jones et al. reference requires only knowledge of the password and possession of the card to access the card contents, which lacks the possession of separate reader and reader memory storing the encryption key that is required to access the flash memory data according to claim 13. And in contrast to the claimed system, the Tatebayashi et al. reference requires possession of the memory card and possession of the reader, which lacks the elements of the means for receiving an access code and means for obtaining the key responsive to that valid access code that is also required to access the encrypted content in the system of claim 13.

---

[39] *Rijckaert, supra; Dembiczak, supra.*

[40] *Fritch, supra; Fine, supra.*

But neither reference indicates any way in which its single-level security is less than adequate. Nor does either reference suggest an additional level of security, by requiring both an access code and a key stored in reader memory, as is necessary to access the flash memory content in the system of claim 13. These substantial differences between the system of claim 13 and the contents of the prior art, and the resulting improvement in security, is indicative of the patentability of claim 13 and its dependent claims.[41]

For these reasons, Appellants submit that the final rejection of claim 13 and each of its dependent claims 17 through 24 is in error and should be reversed.

For the foregoing reasons, therefore, Appellants respectfully submit that the final rejection under §103 of claims 1 through 3, 5 through 8, 11 through 13, and 17 through 24 is in error. Reversal of the final rejection of the claims in this case is therefore respectfully requested.

Respectfully submitted,
/Rodney M. Anderson/
Rodney M. Anderson
Registry No. 31,939
Attorney for Appellants

Anderson, Levine & Lintel, L.L.P.
14785 Preston Road, Suite 650
Dallas, Texas 75254
(972) 664-9554

[41] *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966).

Claims appendix:

1. A method for accessing encrypted information stored in a flash memory storage device, by operating a host system in communication with a reader, the reader including a memory storing a key according to which the information stored in the flash memory storage device is encrypted, the method comprising:

inserting the flash memory storage device into the reader;

forwarding an access code from the host system to the reader;

responsive to the access code being valid for the reader, obtaining the key from the reader; and

decrypting the information stored on the flash memory storage device using the key; and

forwarding the decrypted stored information to the host system.

3. The method of claim 1, further comprising:

encrypting information using the key;

storing the encrypted information in the flash memory storage device; and

removing the flash memory storage device from the reader.

5. The method of claim 1, wherein the access code comprises a first password;

and wherein the obtaining step comprises::

decoding contents stored in the reader to obtain the key from the decoded contents using the first password, responsive to determining that the first password is valid, to obtain the key from the decoded contents.

6. The method of claim 5, further comprising:

comparing the first password to a second password to determine whether the first password matches the second password, wherein the second password is stored in the reader.

7. The method of claim 1, wherein the access code comprises a first password;

and wherein obtaining the key from the adapter includes:

operating the reader to obtain a second password using the first password; and

decoding contents stored in the reader using the second password, responsive to the second password is suitable for decoding the contents associated with the adapter, wherein the contents include the key.

8. The method of claim 1 wherein the reader includes a volatile random access memory (RAM), and wherein the step of obtaining the key includes:

decoding contents stored in the volatile RAM using the access code to obtain the key from the decoded contents.

11. The method of claim 1 wherein the flash memory ~~card~~ storage device is one selected from the group consisting of a secure digital card, a Compact Flash card, a multimedia card, a smart media card, and a Memory Stick card.

12. The method of claim 1 wherein the reader is one of a Universal Serial Bus (USB) reader and a Personal Computer Memory Card International Association (PCMCIA) adapter.

13. A system comprising:

a host system; and

a flash memory reader coupled to the host system, comprising:

an interface for receiving a flash memory storage device,

a reader memory, for storing a key;

circuitry for accessing encrypted information stored in a flash memory device received at the interface, comprising:

means for receiving an access code from the host system, and

means for obtaining the key from the reader memory responsive to the received access code being valid for the reader; and

means for decrypting information stored on a flash memory storage device received at the interface, using the key.

17. The system according to claim 13 wherein the means for obtaining the key comprises:

means for comparing a first password corresponding to the received access code to a second password that is stored in the reader memory; and

means for obtaining the key using the second password responsive to the first password matching the second password.

18. The system according to claim 17 wherein the means for obtaining the key further comprises:

means for obtaining a second password using the first password;

and wherein the means for obtaining the key uses the second password responsive to the second password being suitable for obtaining the key.

19. The system according to claim 17 wherein the reader memory comprises a volatile random access memory (RAM) for storing the received first password,

and wherein the means for obtaining the key comprises:

means for decoding the encoded contents of the reader memory using the first password.

20. The system according to claim 13 wherein the host system is arranged to encrypt information and to write the encrypted information into the memory through the reader.

21. The system according to claim 13 wherein the host is arranged to read information from the memory through the reader and wherein the decrypting means is contained within the host system.

22. The system according to claim 13 wherein the flash memory storage device is a memory card containing a non-volatile memory.

23. The system according to claim 22 wherein the memory card is one selected from the group consisting of a secure digital card, a Compact Flash card, a multimedia card, and a Memory Stick card.

24. The system according to claim 13 wherein the reader is one of a Universal Serial Bus (USB) reader and a Personal Computer Memory Card International Association (PCMCIA) adapter.

Evidence appendix:

None.

Related proceedings appendix:

None.